CLAIMS

1. A method for processing of data that is to be protected, comprising the measure of storing the data as encrypted data element values (DV) in records (P) in a first database (O-DB), each data element value being linked to a corresponding data element type (DT), c h a r a c t e r i s e d by the steps of

storing in a second database (IAM-DB) a data element protection catalogue (DC), which for each individual data element type (DT) contains one or more protection attributes stating processing rules for data element values (DV), which in the first database (O-DB) are linked to the individual data element type (DT),

for each user-initiated measure aiming at processing of a given data element value (DV) in the first database (O-DB), initially producing a compelling calling to the data element protection catalogue for collecting the protection attribute/attributes associated with the corresponding data element type, and

compellingly controlling the user's processing of the given data element value in conformity with the collected protection attribute/attributes.

2. A method as claimed in claim 1, further comprising the measure of storing the protection attribute/attributes of the data element protection catalogue (DC) in encrypted form in the second database (IAM-DB) and, when collecting protection attribute/attributes from the data element protection catalogue (DC) effecting decryption thereof.

3. A method as claimed in ~~any one of the preceding claims,~~ claim 1 wherein each record (P) in the first database (O-DB) has a record identifier, and wherein the method further comprises the measure of storing the record identifier in encrypted form (SID) in the first database (O-DB).

4. A method as claimed in ~~any one of the preceding claims~~, wherein the encryption of data in the first database (O-DB) and/or the encryption of data in the second database (IAM-DB) is carried out in accordance with the PTY principle with floating storage identity.

5. A method as claimed in ~~any one of the preceding claims~~, wherein the protection attribute/attributes of the data element types comprise attributes stating rules for encryption of the corresponding data element values in the first database (O-DB).

6. A method as claimed in ~~any one of the preceding claims~~, wherein the protection attribute/attributes of the data element types comprise attributes stating rules for which program/programs or program versions is/are allowed to be used for managing the corresponding data element values in the first database (O-DB).

7. A method as claimed in ~~any one of the preceding claims~~, wherein the protection attribute/attributes of the data element values comprise attributes stating rules for logging the corresponding data element values in the first database (O-DB).

8. An apparatus for processing data that is to be protected, comprising a first database (O-DB) for storing said data as encrypted data element values (DV) in records (P), each data element value being linked to a corresponding data element type (DT), c h a r a c - t e r i s e d by

a second database (IAM-DB) for storing a data element protection catalogue (DC), which for each individual data element type (DT) contains one or more protection attributes stating processing rules for data element values (DV), which in the first database (O-DB) are linked to the individual data element type (DT),

means which are adapted, in each user-initiated measure aiming at processing a given data element value (DV) in the first database (O-DB), to initially produce a compelling calling to the data element protection cata-

logue for collecting the protection attribute/attributes associated with the corresponding data element types, and

means which are adapted to compellingly control the user's processing of the given data element value in conformity with the collected protection attribute/attributes.

A00 C5